ИНФОРМАЦИОННЫЕ СИСТЕМЫ.

СРЕДСТВА, ТЕХНОЛОГИИ, БЕЗОПАСНОСТЬ

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ .NET REMOTING ДЛЯ РЕШЕНИЯ ЗАДАЧИ ПОИСКОВОЙ ОПТИМИЗАЦИИ

А.Ю.Горбунов

Нижегородский госуниверситет

Задача оптимизации состоит в нахождении наибольшего или наименьшего значения некоторой функции $F(X)$ (целевой функции) на заданном множестве $X \subseteq D$ (области поиска). На настоящий момент опубликовано большое количество методов решения поставленной задачи для случая линейной целевой функции и небольшого размера области поиска. К сожалению, для большинства практических задач данные условия неприменимы. Поставленную задачу предлагается решать на основе методов адаптивного поиска (например, используя генетические алгоритмы, широко описанные в литературе [1,2]). Поскольку целевая функция в общем случае является многоэкстремальной, то необходимо использовать несколько процедур поиска (спусков) для нахождения оптимального решения. Ввиду потенциально большого размера области поиска имеет смысл проводить процедуры спуска параллельно на нескольких ЭВМ.

Данная задача может быть эффективно решена с помощью технологии .NET Remoting [3,4]. .NET Remoting предоставляет простой и прозрачный для пользователя способ взаимодействия объектов через границу домена приложения. Технология является гибкой в эксплуатации, позволяет задействовать различные варианты настроек удаленных объектов и использовать различные транспортные протоколы (TCP, HTTP) и протоколы доступа к объектам (SOAP, бинарный формат). Последнее обстоятельство полезно при работе в сетях со сложной топологией, использующих межсетевые экраны.

На настоящий момент разработана программная система, реализующая решение поставленной задачи [4]. Система разбита на три модуля – сервер, клиент и модуль вычисления целевой функции (калькулятор). В задачи сервера входит публикация удаленного объекта, сообщающего клиенту при подключении параметры области поиска (задается в виде файла в формате XML на стороне сервера) и полное имя сборки, содержащей калькулятор. Калькулятор реализует интерфейс, известный клиенту. Сборка, содержащая калькулятор, хранится на стороне сервера и при подключении копируется на машину клиента. Клиент, получив параметры области поиска и подключив, используя динамическое связывание, калькулятор, производит процедуру спуска и возвращает найденное решение на сервер. Сервер на основе найденных клиентами решений производит дополнительную процедуру

спуска и сохраняет найденное решение в файле. Предложенная архитектура системы позволяет производить замену параметров области поиска и калькулятора без перекомпиляции клиента и сервера, то есть без каких-либо усилий настраивать систему под решение конкретной задачи. Использование конфигурации клиента с помощью конфигурационных файлов избавляет от необходимости перекомпиляции кода клиентов при смене местоположения сервера.

На стороне клиента для поиска используется локальный поисковый метод на основе генетических алгоритмов, поскольку это ускоряет процедуру спуска и избавляет от необходимости передавать клиенту реализации глобальных поисковых методов. Использование глобального поискового метода на стороне сервера повышает надежность, а использование в качестве исходных данных найденных клиентами локальных решений уменьшает общее время поиска (тем самым, повышая эффективность).

Эффективность поиска предложенной системой определяется используемыми поисковыми методами. Высоких показателей эффективности можно достичь при использовании глобального поиска на сервере и быстрого локального на стороне клиентов.

Надежность поиска также зависит от используемых поисковых методов и возрастает при увеличении числа клиентов. Надежность сильно зависит от размера области поиска и характера целевой функции.

Точность поиска полностью определяется используемыми поисковыми методами. Для генетических алгоритмов

$$\Delta X = \frac{|D|}{2^L}$$

где $|D|$ – мощность множества области поиска, L – длина бинарной строки, представляющей найденное решение (длина генотипа).

Разработанная программная система может быть использована как при проведении научных исследований, так и в учебном процессе для обучения студентов основам построения распределенных систем и основам методов поисковой оптимизации.

[1] Goldberg D.E. Genetic Algorithms in Search, Optimization, and Machine Learning. Addison-Wesley, Reading, MA, 1989.
[2] Holland J.H. Adaptation in Natural and Artificial Systems. MIT Press, Cambridge, MA, 2nd edition, 1992.
[3] Маклин С., Нафтел Дж., Уильямс К. Microsoft .NET Remoting. –М.: Русская редакция, 2003.
[4] Горбунов А.Ю. //В кн.: Технологии Microsoft в теории и практике программирования: Тезисы конференции студентов, аспирантов и молодых ученых: Москва, 4-5 марта 2004 /Сост. Б.И. Березин, С.Б. Березин. –М.: Издательский отдел факультета вычислительной математики и кибернетики МГУ им. М.В. Ломоносова, 2004. с.11

ОБНАРУЖЕНИЕ DOS И DDOS АТАК МЕТОДОМ СКОЛЬЗЯЩЕГО ОКНА

А.А.Борисов, Л.Ю.Ротков, А.А.Рябов

Нижегородский госуниверситет

В наши дни атаки компьютерных сетей типа “отказ в обслуживании” (DoS, Denial of Service) являются одними из наиболее распространенных видов атак. Частично виной тому является простота их реализации и высокая эффективность. Побочным эффектом таких атак является большой трафик, направленный на атакуемый ресурс, что часто игнорируется сетевыми администраторами, и принимается за обычное поведение сетевого сегмента или атакуемого сервера.

Основные типы DoS атак: блокировка канала связи и блокировка сетевого сервиса.

На сегодняшний день не известно средство, гарантирующее полную защиту от DoS атак. Поэтому актуальна проблема разработки механизмов обнаружения DoS атак.

Разделим DoS атаки на две группы. К первой группе относятся атаки, при которых используются сетевые пакеты одинаковой длины. Ко второй отнесем атаки, при которых длина пакета – случайная величина в заданном интервале.

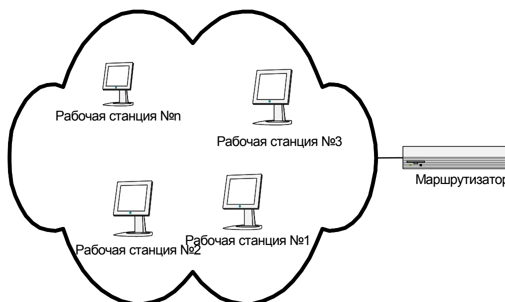


Рис 1

Для исследования возможности обнаружения DoS атак был проведен эксперимент в системе, изображенной на рис.1, представляющей собой сегмент компьютерной сети факультета. При этом сеть работала в обычном режиме и подвергалась воздействию атакой.

С помощью генератора трафика создавались атаки 1-ой и 2-ой группы. Для обнаружения атак применялся метод скользящего окна [1]. Атака 1-ой группы была обнаружена менее чем за 1с. Атаку 2-й группы обнаружить не удалось. Следовательно, для обнаружения таких атак необходимо искать другой метод.

Рассмотрим изменение энтропии системы при использовании в ней различных сочетаний длин пакетов. Энтропия системы определяется соотношением

$$S_n = -\sum_{i=\min}^{\max} P_i \log_2 P_i \,, \qquad (1)$$

где n – возможное число вариантов длин, P_i – вероятность появления в канале передачи данных пакета длиной i байт, min – минимальное значение длины пакета, max – максимальное значение длины пакета.

При отсутствии атаки энтропия системы при больших n примерно постоянная величина, равная 4.

На рис.2 приведена кривая изменения энтропии в зависимости от длины передаваемых сетевых пакетов. Из рисунка видно, что при увеличении числа n энтропия системы при воздействии атакой 1-ой группы быстро стремится к 0. Это выделяет DoS атаку 1-ой группы из процессов, происходящих в сети. На рис.3 изображена энтропия для DoS атаки 2-ой группы. Видно, что энтропия также стремится к 0, но медленнее, чем в первом случае. Это связано с тем, что эта DoS атака осуществлялась потоком сетевых пакетов случайной длины, равномерно распределенной на некотором интервале.

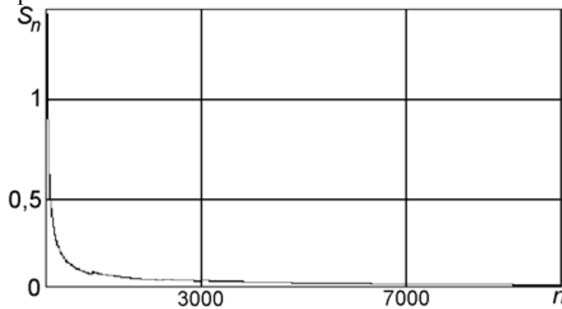


Рис 2

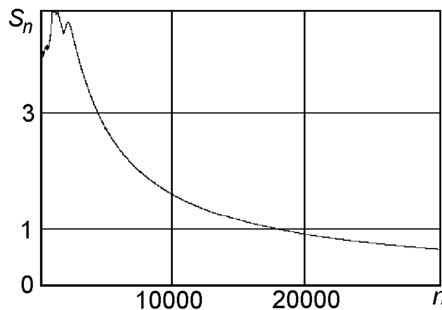


Рис 3

Таким образом, можно предположить, что сравнением кривых для случаев “типичного” (отсутствие атаки) и смешанного (наличие атаки на фоне “типичного”) трафиков можно обнаружить наличие атаки.

[1] Борисов А.А., Ротков Л.Ю. //В кн.: Тр. 6-й научн. конф. по радиофизике, посвященной 100-летию со дня рождения М.Т.Греховой. 7 мая 2002 г. /Ред. А.В.Якимов. –Н.Новгород: ТАЛАМ, 2002. С.306.

ОЦЕНКА ЗАДЕРЖЕК СООБЩЕНИЙ В ПОДВИЖНОЙ СТАНЦИИ СТАНДАРТА GSM

Н.В.Глазов, Е.С.Золотницкий

Нижегородский госуниверситет)

Актуальность исследования величины задержек сообщений в сетях сотовой связи обусловлена широким распространением сетей GSM. Знание значений задержек позволит более точно настроить эхокомпенсаторы и эходавители, и тем самым улучшить качество связи.

Одним из устройств, вносящим значительную задержку, является подвижная станция (ПС). Задержка сигнала при передаче речи в полноскоростном режиме работы ПС в направлении “вверх” – это задержка между акустическим моментом в Микрофоне и последним битом соответствующего речевого фрейма в антенном коннекторе. Полноскоростная речевая задержка в ПС в направлении “вниз” – это задержка между первым битом речевого фрейма в антенном коннекторе и последним акустическим моментом в Динамике, соответствующим этому речевому фрейму.

Подвижную станцию можно представить состоящей из блока управления, приёмо-передающего блока и антенного блока. Для вычисления задержки сигнала в ПС интересен приёмо-передающий блок.

Существует серия стандартов ETSI на задержку сигнала при прохождении ПС [1,2]. По стандарту, полноскоростная задержка в направлении “вверх” не должна превышать 72,1 мс. Она складывается из: 2 мс задержки на АЦП, 20 мс задержки на сегментирование речи, 8 мс, требующихся кодеру для обработки речи от входа последнего ИКМ сэмпла до выхода конечного кодированного бита, 1,6 мс, требующихся канальному кодеру для осуществления канального кодирования, 3,0 мс допусков для системных событий, которые являются системозависимыми, и 37,5 мс, требуемых для передачи фрейма по радиоканалу из-за перемежения и деперемежения. Стоит отметить, что это лишь верхние границы величин задержек.

Основное влияние на формирование задержки, если не говорить про перемежение, оказывает кодер речи. Кодер речи сделан по принципу кодирования источника сигнала. Метод кодирования источника сигнала основывается на данных о механизме речеобразования и реализуется в вокодерах. В сотовой связи используются вокодеры на основе линейного предсказания (ЛП). Кодирование речи на основе ЛП заключается в том, что по линии связи передаются не параметры речевого сигнала, а параметры фильтра, эквивалентного голосовому тракту, и параметры сигнала возбуждения этого фильтра.

На рисунке изображена упрощенная блок-схема кодера речи в стандарте GSM. Блок предварительной обработки осуществляет разбиение сигнала на 20 мс сегменты. Далее, для каждого 20 мс сегмента оцениваются параметры фильтра кратковременного ЛП (фильтра выделения формант). Сигнал с выхода блока предварительной обработки фильтруется фильтром-анализатором кратковременного ЛП. Выходной сигнал разбивается на 5 мс сегменты и идёт на оценку параметров фильтра дол-

говременного предсказания (ДП), а также фильтруется анализатором ДП. По остатку последнего формируются параметры сигнала возбуждения для каждого 5 мс сегмента в отдельности. Алгоритмы оценки параметров фильтров и сигнала возбуждения известны и описаны в [3].



Работу речевого кодера в мобильной станции можно представить в виде совокупности простых операций, таких как сложение, умножение, отрицание, сравнение. Так как время кодирования сильно зависит от самого сигнала, то во всех случаях ветвления берутся варианты с наибольшим числом операций. В итоге получается, что речевой кодер при обработке одного речевого фрэйма производит ~4000 сложений, ~3000 умножений и ~4000 операций сравнения.

В результате имеем число простых операций, совершаемых речевым кодером при обработке одного речевого фрэйма. Развитием работы может служить нахождение количества операций, совершаемых кодером канала при перемежении.

[1] ‘Digital cellular telecommunications system (Phase 2+); Technical performance objectives’; European Telecommunications Standards Institute, GSM 03.05 version 8.0.0 Release 1999.
[2] ‘Digital cellular telecommunications system (Phase 2+); Transmission planning aspects of the speech service in the GSM Public Land Mobile Network (PLMN)’; European Telecommunications Standards Institute, GSM 03.50 version 8.1.1 Release 1999.
[3] ‘Digital cellular telecommunications system (Phase 2+); Full rate speech; Transcoding (Release 99)’; European Telecommunications Standards Institute, GSM 06.10 version 8.2.0 Release 1999.

ПРИМЕНЕНИЕ НЕЙРОСЕТЕЙ АРТ ДЛЯ ЭХО КОМПЕНСАЦИИ

Е.С.Золотницкий, А.Е.Комлев

Нижегородский госуниверситет

В современных сетях цифровой сотовой телефонии образуются задержки в передаче сигнала, сравнимые с задержками при межконтинентальных переговорах. В сетях сотовой подвижной связи задержка возникает на различных этапах распространения сигнала. Несогласованность различных элементов наземной инфраструктуры оператора связи приводит к возникновению эха, т.е. отражённого сигнала, который в зависимости от некоторых условий может серьёзно ухудшить качество связи или сделать её невозможной. С учётом особенностей GSM сетей (цифровые методы передачи информации, внесённые в стандарты, и временные допуски на задержку сигнала), можно воспользоваться цифровыми методами уменьшения вредного воздействия эха, применив для этой цели нейронные сети Адаптивной Теории Резонанса (АРТ). Сети и алгоритмы АРТ сохраняют пластичность, необходимую для изучения новых образов, в то же время предотвращая изменение ранее запомненных образов [1].

Сеть АРТ представляет собой векторный классификатор. Входной вектор классифицируется в зависимости от того, на какой из множества ранее запомненных образов он похож. Своё классификационное решение сеть АРТ выражает в форме возбуждения одного из нейронов распознающего слоя. Если входной вектор не соответствует ни одному из запомненных образов, создаётся новая категория посредством запоминания образа, идентичного новому входному вектору. Если определено, что входной вектор похож на один из ранее запомненных векторов с точки зрения определенного критерия сходства, запомненный вектор будет изменяться (обучаться) под воздействием нового входного вектора таким образом, чтобы стать более похожим на этот входной вектор. Таким образом, решается дилемма стабильности-пластичности [1].

Устанавливать нейронную сеть имеет смысл на границах сопряжения с кабельными сетями.

Реализация блока распознавания, содержащего нейронную сеть, возможна тремя следующими способами.

1. Для работы используются две нейронных сети. На вход первой поступает поток информации от точки А, который непосредственно перед сетью разбивается линией задержки на блоки длительностью Δt. Обрабатывая этот поток, сеть формирует образы. Вторая сеть дублирует структуру первой и одновременно использует созданные ей образы. На её вход поступает информационный поток от точки В, разбитый на блоки линией задержки. Сеть ищет сходство с образами, сформированными первой сетью.



2. Вместо первой

нейронной сети можно использовать некий блок преобразования, который будет непосредственно формировать рабочие образы для второй сети. Данный вариант имеет преимущество по вычислительным затратам.

3. Во всей схеме можно использовать одну нейронную сеть, которая будет переключаться между двумя режимами. В режиме обучения поток информации от точки А, проходя линию задержки, будет подаваться на вход сети, и на его основе будут формироваться образы для последующей работы. В это время поток от точки В буферизуется. После формирования достаточного количества образов сеть переключается в режим обработки сигнала. Теперь уже буферизуется поток от точки А, а поток от точки В, проходя линию задержки, поступает на вход сети для сравнения. Данная реализация внесет большую задержку в работу, чем две предыдущие, т.к. потребуется время на буферизацию и переключение сети.

После распознавания эха нейронной сетью необходимо будет удалить его из сигнала. Для этого вычитается нормированный по мощности запомненный образ. В результате такой обработки значительно уменьшается уровень эха в сигнале. Но, в тоже время, нужно найти некий баланс между размером (длительностью образа) и качеством подавления эха. Если образ велик – сеть легче находит сходство с ним, т.к. велик объем информации и вероятность неверного совпадения мала, но при этом некачественна “послесетевая” обработка сигнала. Если же образ мал, то обрабатывать его достаточно легко, но велика вероятность неправильного опознавания.

Возможность внедрения нейронной сети в сеть сотовой связи определяется следующим неравенством:

$$\Delta t_1 + t_{\text{Иниц.Ср1}} + n_1(t_{\text{расп1}} + t_{\text{Ср1}} + t_{\text{сбр1}} + t_{\text{общ.обр1}}) + t_{\text{сравн.1}} + t_{\text{норм.1}} + t_{\text{вычит.1}} + t_{\text{общ.затрат1}} +$$
$$+ \Delta t_2 + t_{\text{Иниц.Ср2}} + n_2(t_{\text{расп2}} + t_{\text{Ср2}} + t_{\text{сбр2}} + t_{\text{общ.обр2}}) + t_{\text{сравн.2}} + t_{\text{норм.2}} + t_{\text{вычит.2}} + t_{\text{общ.затрат2}} +$$
$$t_{\text{ISDN}} \leq 400 \text{ мс}.$$

Здесь $t_{\text{сравн.}}$ – время на определение мощности эха по сравнению с исходным сигналом, $t_{\text{норм.}}$ – время на нормирование мощности, $t_{\text{вычит.}}$ – время удаления образа из сигнала, $t_{\text{общ.затрат}}$ – время на внутреннюю обработку, Δt – длительность образа сети. $t_{\text{Иниц.Ср}}$ – время инициализации слоя сравнения, $t_{\text{расп}}$ – время обработки сигнала в слое распознавания, $t_{\text{Ср}}$ – время обработки в слое сравнения, $t_{\text{сбр}}$ – время сравнения в блоке сброса, $t_{\text{общ.обр.}}$ – время обработки сигнала на остальных шагах работы. Значение задержки в 400 мс взято из стандарта ETSI GSM 03.50.

Таким образом, вся обработка сигнала нейронной сетью и послесетевая обработка сигнала по удалению найденного эха должна укладываться во временные рамки, заданные существующими стандартами GSM. В процессе работы сети можно также динамически корректировать параметры сети (коэффициент подобия, длительность образа сети, количество циклов шагов в цикле распознавания). Таким образом, можно достигнуть максимального качества эхо компенсации.

[1] Carpenter O., Grossberg S. 1987 ART-2: Self-organization of stable category recognition codes for analog input patterns. Applied Optics 26(23):4919-30.

ИССЛЕДОВАНИЕ МЯГКИХ ХЭНДОВЕРОВ В СЕТЯХ GSM

Е.С.Золотницкий, А.Е.Литвинов

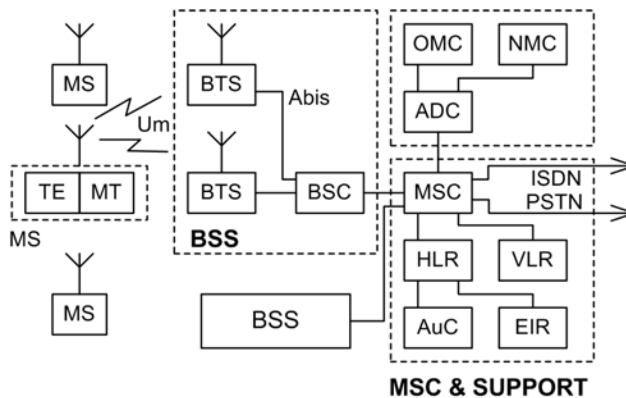
Нижегородский госуниверситет

В современных сетях GSM основным источником обрывов связи является хэндовер (эстафетная передача абонента от одной соты в другую). В большинстве случаев это результат плохой настройки сети, а так же нерационального радиопокрытия. Однако проблема обрывов связи при хэндовере остаётся и при грамотной настройке оборудования.

В Европе существует проблема хэндоверов на линиях высокоскоростных поездов. Скорость таких поездов держится на отметке 250 км/ч. Установка вдоль путей обычного городского оборудования базовых станций не обеспечивает удачное завершение процедуры хэндовера. Требуется установка дорогостоящего оборудования базовых станций и антенно-фидерных систем.

Предлагаемый метод основывается на уже существующем способе передачи абонентов сотами в сетях CDMA. Это мягкий режим хэндовера.

В сетях GSM хэндовер осуществляется жёстко (т.е. с временным разрывом соединения), но теоретически можно часть из них проводить мягко (без разрыва). Это можно осуществить, подготовив в новой соте свободный канал на той же частоте с тем же временным слотом. Также нужно следить за отсутствием интерференции и динамическим перевыделением каналов. Такой приём будет эффективнее работать в сети с небольшими нагрузками [1]. В корректно спроектированной сети избыточность числа обрабатывающих каналов присутствует большую часть времени. Эту избыточность можно использовать. Оценочные расчёты показывают, что при введении данного метода есть возможность избежания каждого четвертого обрыва радиосоединения. Но самое главное, метод позволяет проводить мягкие хэндоверы на высокоскоростных железнодорожных линиях, используя обычное городское станционное оборудование.



Изучение инфраструктуры сети GSM показало, что метод можно ввести без существенных изменений в сети. Требуется изменение обслуживающего программного обеспечения, присутствующего в каждой аппаратной единице сети GSM.

Управление и

наблюдение за сетью проводится в специальной подсети OMC-R [2], в которую требуется интеграция задач, отвечающих за проведение мягких хэндоверов. В процедуре принятия решения о проведении хэндовера рассматриваемый метод не участвует. Его задача – принять решение о способе проведения хэндовера. На входе системы имеется заявка сети на перевод абонента в новую соту, а также ряд параметров абонента, исходя из которых решается задача возможности проведения мягкого хэндовера.

В качестве параметров с мобильной станции используются: RXLEV_DL (уровень приёма собственной соты), RXQUAL_DL (величина ошибок двоичного разряда канала собственной соты), RXLEV_NCELL (уровень приема сигнала соседних сот), уровень приема сигнала соседних сот, BSIC_NCELL(идентификаторы соседних сот). Параметры, полученные с базовой станции: RXLEV_UL (мобильной станции), RQUAL_UL (величина ошибок двоичного разряда сигнала, передаваемого мобильной станцией). Измерения проводятся каждый раз по полному мультикадру SACCH, т.е. в течение 480 мс [3]. На основе этих данных рассчитывается физическое место положения станции [4].

Для расчета требуется знать карту частот и каналов, которая есть у оператора. На основе собранной информации, система просчитывает необходимость и возможность проведения мягких хендоверов, затем создаёт новые каналы и принимает решения о судьбе старых каналов.

Для создания/удаления частот, то есть для изменения частотного плана, существует процедура RFPC (Radio Frequency Plan Change), с помощью которой система создаёт новые частоты. В случае возможности проведения мягкого хэндовера, управление хэндовером переходит к данной задаче. Передача абонента будет проходить с помощью процедуры FH (Force Handover), которая позволяет в ручную перевести абонента в новую соту, на нужную частоту и нужный временной слот.

Таким образом, путем незначительных изменений программного обеспечения мобильной станции, базовой станции, базового контроллера и управляющего центра можно устранить часть обрывов связи в городском режиме и полностью избежать обрывов на высокоскоростных железнодорожных путях и автомагистралях.

[1] Золотницкий Е.С., Литвинов А.Е., Ротков Л.Ю. //В кн.: Тр. 7-й научн. конференции по радиофизике. 7 мая 2003 г. /Ред. А.В.Якимов. –Н.Новгород: ТАЛАМ, 2003, с.293.
[2] GSM, cdmaOne and 3G Systems. Raymond Steele, Chin-Chun Lee and Peter Gould, 2001 John Wiley & Sons Ltd.
[3] GSM 05.08 (ETS 300 578) European Digital Cellular Telecommunications System (Phase 2); Radio Subsystem Link Control.
[4] GSM 05.05 (ETS 300 577), European Digital Cellular Telecommunications System (Phase 2); Radio Transmission and Reception.

О ПРИВЕДЕНИИ МАТРИЦ К КАНОНИЧЕСКОМУ ВИДУ В ПРОИЗВОЛЬНОМ ПОЛЕ

К.Г.Кирьянов, А.В.Милютин

Нижегородский госуниверситет

Исключительные свойства и экономичность генераторов псевдослучайных последовательностей (ГПСП) определили весьма широкие области их применения при решении задач кодирования и связи [1]. Последнее время рассматриваются свойства синхронизация ГПСП [2,3] и для целей криптографии. Ранее в работах других авторов [1] свойства синхронизации ГПСП не рассматривались. В [2] предложена математическая модель (ММ) связанных ГПСП $y(t+1) = M \times y(t)$, $y(0)=y_0$, требующая для анализа трудоёмкой операции приведения системной (n·n) матрицы M к каноническому виду K в поле GF(q) заменой $x(t) = P \times y(t)$. При этом $x(t+1) = P \times M \times P^{-1} \times x(t) \equiv M_1 \times x(t)$. Полагается, что P^{-1} существует. В настоящей работе реализована программа приведения матрицы M в полях GF(q), q∈[2,3,5,7,11,13] и кольцах GR(q), q∈[2,…,16] при n∈[2,…,64]. В технике чаще используется q=2. Канонический вид – матрица

$$K = \begin{vmatrix} f_1(\lambda) & 0 & \dots & 0 & 0 \\ 0 & f_2(\lambda) & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & f_{n-1}(\lambda) & 0 \\ 0 & 0 & \dots & 0 & f_n(\lambda) \end{vmatrix},$$

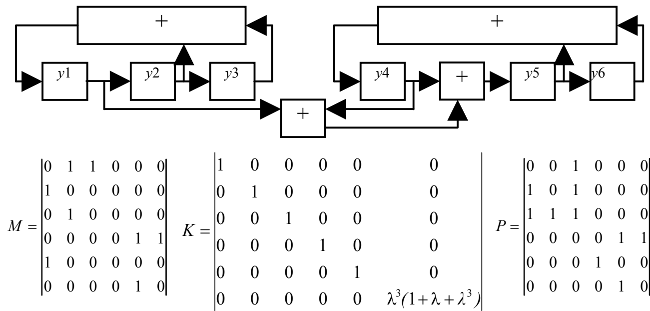
где многочлены $f_1(\lambda), f_2(\lambda),\dots,f_n(\lambda)$ определяются путем применения алгоритма для любого поля из ([1]-[4]) к матрице $K = \lambda \times I - M_1$ (где I – единичная матрица). Далее приводятся примеры. **Пример 1** – тестовый, взят из [1].

$$M = \begin{vmatrix} 0&0&1&1&1&1&1&1 \\ 0&1&0&0&0&0&0&0 \\ 0&1&1&1&1&1&1&1 \\ 0&0&0&0&1&1&1&1 \\ 0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&1&0&1 \\ 0&0&0&0&0&0&1&1 \\ 0&0&0&0&0&0&1&0 \end{vmatrix} \quad K = \begin{vmatrix} 1&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0 \\ 0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&1+\lambda&0&0 \\ 0&0&0&0&0&0&(1+\lambda)\lambda&0 \\ 0&0&0&0&0&0&0&(1+\lambda)^2\lambda(1+\lambda+\lambda^2) \end{vmatrix}$$

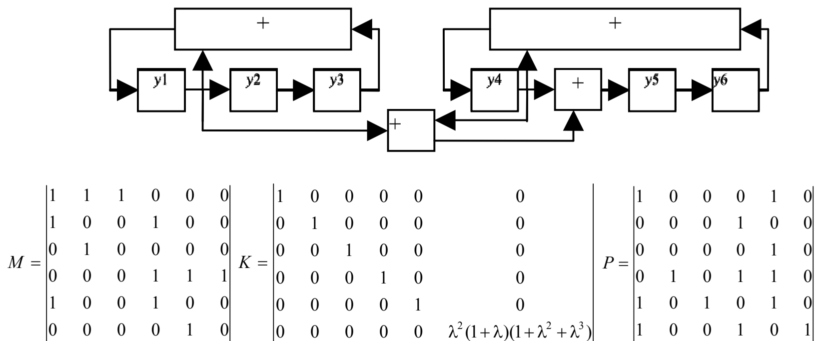
Инвариантные множители матрицы K:

$$f_1(\lambda) = 1; f_2(\lambda) = 1; f_3(\lambda) = 1; f_4(\lambda) = 1; f_5(\lambda) = 1; f_6(\lambda) = 1 + \lambda; f_7(\lambda) = (1 + \lambda)\lambda;$$
$$f_8(\lambda) = (1 + \lambda)^2\lambda(1 + \lambda + \lambda^2).$$

Примеры 2 и 3 с “абсолютной” и “условной” (не при всех начальных условиях y_0) синхронизацией связанных генераторов ПСП [2].



$$M = \begin{vmatrix} 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{vmatrix} \quad K = \begin{vmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & \lambda^3(1+\lambda+\lambda^3) \end{vmatrix} \quad P = \begin{vmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{vmatrix}$$



$$M = \begin{vmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{vmatrix} \quad K = \begin{vmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & \lambda^2(1+\lambda)(1+\lambda^2+\lambda^3) \end{vmatrix} \quad P = \begin{vmatrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 \end{vmatrix}$$

Работа выполнена при частичной поддержке РФФИ (грант 02-02-17573).

[1] Гилл А. Линейные последовательностные машины. Анализ, синтез и применение. -М.: Наука, 1974.
[2] Кирьянов К.Г., Меднов А.С., Акулов В.В. Синхронизация генераторов псевдослучайных последовательностей. //Техника средств связи. “ЭКОС”. 1990. Сер. РИТ. Вып. I. С.56.
[3] Bagrov S.N., Kirjanov K.G., Shalfeev V.D. Complicated Regimes. Synchronization and Structures in Networks of the Pseudo-Random Generators. //Dynamic and Stochastic Wave Phenomena. Abstracts of the Second International Scientific School-Seminar. -N-Novgorod: Nizhny Novgorod University Press, 1994.
[4] Гантмахер Ф.Р. Теория матриц. -М., 1967, с.159.

ГИПОТЕТИЧЕСКАЯ КРИПТОСИСТЕМА УНИВЕРСАЛЬНОГО ГЕНЕТИЧЕСКОГО КОДИРОВАНИЯ

К.Г.Кирьянов, М.А.Нечуев

Нижегородский госуниверситет

Из многочисленных публикаций и работ ведущих организаций и фирм [1] становятся очевидны многие новые актуальные проблемы в области генетики, биофизики и, в частности, в области дальнейших исследований математических моделей компьютерной генетики в части приложений к задачам радиофизики и информатики. В настоящее время в техногенных системах защиты информации все более широкое распространение получают различные системы кодирования и шифрования. В объектах живой природы для целей шифрования и кодирования наследственной информации используется принцип, известный как т.н. Универсальное Генетическое Кодирование-Шифрование (УГК/УГШ). Наследственная информация, хранящаяся в молекулах ДНК, различна для всех организмов, принципы же УГК являются инвариантными для всей живой материи. УГК основано на отображении (трансляции) 64-х 3-символьных элементов – кодонов: $X_1X_2X_3$ (где X_i является одним из 4-х азотистых оснований – нуклеотидов {***u***, ***c***, ***a***, ***g***}, i = 1,2,3) в 21 аминокислоты, которые затем синтезируются в белок. Генетический текст (последовательность нуклеотидов) получается в результате секвенирования генома, которое в СМИ обычно называется "расшифровкой генома".

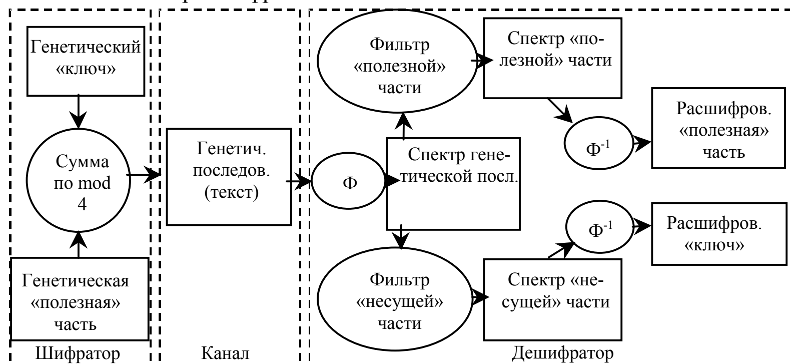


Рис. 1

Существуют разные подходы к пониманию механизма работы УГК [2]. В данной работе рассматривался криптологический принцип организации УГК. Модель исследования представлена на рис.1. Под "шифратором" понимается предполагаемый природный механизм шифрования полезной информации. "Канал" – носители генетической информации (молекулы ДНК). "Доступ к каналу" осуществляется с

помощью секвенирования. Операции Ф и $Ф^{-1}$ являются соответственно прямым и обратным преобразованием Фурье.

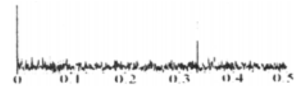


Рис. 2

Четкий пик в спектре генетического текста (ГТ) на относительной частоте 0,333 или периоде T=3, равном размеру кодона (рис.2), наблюдается на участках, кодирующих белок. Число три можно интерпретировать как период "несущей частоты" в данных участках. С помощью прямоугольного фильтра, наложенного на спектр ГТ, были восстановлены "полезная" и "ключевая" части, последняя из которых оказалась трехуровневой. Непрерывность "несущей" по уровню в сочетании с тем фактом, что количество нуклеотидов равно четырем, не позволила однозначно идентифицировать "несущую" (или ключ). Тем не менее, данный подход дает информацию об относительном расположении элементов ключа (нуклеотидов). Таким образом, из множества всех возможных ключей были отобраны: **UCA AUC UCG AGU UAG AGC CAU GUC CAG GUA CGU GCA.**

С целью уточнения ключа было произведено "декодирование" исходного генетического текста всеми возможными ключами-кодонами (от текста отнимался по модулю 4 периодически повторенный кодон) и сравнение спектров получившихся 64-х последовательностей. Кодонов, "правильно" декодирующих исходный генетический текст, т.е. максимально снижающих уровень пика в спектре до уровня боковых шумоподобных составляющих, оказалось три: **UCA**, **UGA** и **ACA**. Теперь можно видеть, что единственно возможным ключом можно считать тройку **UCA,** так как только этот кодон присутствует в списке "кандидатов в ключи", полученном выше.

В рамках рассматриваемой в настоящей работе модели, после декодирования ключом **UCA** участков генетического текста получена приведенная здесь таблица-словарь, совпадающая с таблицей УГК по числам заполнения строк (синонимичности), но отличающаяся по наполнению.

кодон	**а/к**
uga ugg	F
ugu ugc cgu cgc cga cgg	L
uuu uuc uua uug aaa aag	S
uca ucg	Y
uaa uag	C
uac	W
cuu cuc cua cug	P
cca ccg	H
ccu ccc	Q
cau cac caa cag aau aac	R
agu aga agg	I
agc	M
auu auc aua aug	T
aca acg	N
acu acc	K
ggu ggc gga ggg	V
guu guc gua gug	A
gca gcg	D
gcu gcc	E
gau gac gaa gag	G
ucu ucc uau	stop

Результаты исследований, по нашему мнению, вносят определенный вклад в создание модели гипотетической криптосистемы для ещё не полностью изученной динамики системы Универсального Генетического Кодирования.

Работа выполнена при частичной поддержке РФФИ (грант 02-02-17573).

[1] Киселев Л.Л. //Вестник Российской Академии Наук. 2000. Т.70,№5. С.412.
[2] Кирьянов К.Г. Генетический код и тексты: динамические модели сложных систем. -Нижний Новгород: ТАЛАМ, 2002, 100с.

ОЦЕНКА ПОГРЕШНОСТИ ИЗМЕРЕНИЯ ОТНОСИТЕЛЬНОЙ ОТСТРОЙКИ ЧАСТОТЫ ВЫСОКОСТАБИЛЬНЫХ ГЕНЕРАТОРОВ ПРИЕМНИКОМ-КОМПАРАТОРОМ СИГНАЛОВ СРНС ГЛОНАСС/GPS

В.В.Акулов, Р.Н.Новожилов

ФГУП ННИПИ “Кварц”

Приемник-компаратор (ПК) предназначен для сличения частоты внутреннего или внешнего высокостабильного генератора с эталонной частотой, передаваемой по радиоканалу. Наряду с ПК ДВ диапазона ПК ГЛОНАСС/GPS является важным звеном в обеспечении метрологической автономности поверочных комплексов, позволяя производить сличение и поверку частоты опорного генератора (ОГ) без использования более точных стандартов, например, водородных.

В ПК ГЛОНАСС/GPS реализован фазововременной метод (ФВМ) определения отстройки частоты ОГ, т.е. относительная отстройка частоты определяется по набегу фазы, отнесенной к времени измерения (T). Пусть датчик ГЛОНАСС передает сигнал на ИИВ в виде $G(t) = g_0 + g(t)$, где g_0 – эталонное значение частоты 1Гц, $g(t)$– случайный процесс флуктуации частоты датчика. Поверяемый стандарт передает сигнал с частотой 1Гц в виде $F(t) = f_0 + f_1(t) + f_2(t)$, где f_0 – эталонное значение частоты генератора, $f_1(t)$ – процесс систематического ухода частоты, $f_2(t)$-случайный процесс флуктуации частоты ОГ с нулевым средним значением. На рис.1 показана структурная схема определения набега фазы между двумя измерениями. В соответствии с этой схемой можно записать общее выражение для набега фазы:

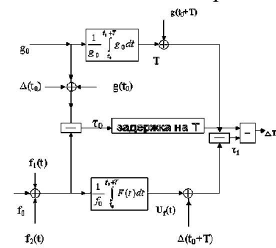


Рис. 1

$$\Delta T(t) = \frac{1}{f_0} \int_{t_0}^{t_0+T} (f_1(t) + f_2(t))\,dt + \Delta(t_0 + T) + g(t_0 + T) - \Delta(t_0) - g(t_0), \qquad (1)$$

где $\Delta(t)$ – ошибка, вносимая датчиком ГЛОНАСС.

Пренебрегая систематическим уходом частоты и ошибкой, вносимой датчиком ГЛОНАСС, можно оценить случайную составляющую ошибки опорного генератора. Зная спектральную плотность мощности процесса $f_1(t)$ [1], запишем выражение для дисперсии погрешности:

$$\sigma_{t_1}^2(T) = \langle |\Delta t_1(T)|^2 \rangle = \frac{T^2}{f_0^2} \langle \left[\frac{1}{T} \int_{t_0}^{t_0+T} f_1(t)\,dt \right]^2 \rangle = \frac{2T^2}{f_0^2} \int_0^{\infty} S_f(\omega) \frac{\sin^2 \frac{\omega t}{2}}{(\frac{\omega t}{2})^2} d\omega . \qquad (2)$$

Рассмотрим несколько частных случаев случайной составляющей отклонения частоты: а) гармонический процесс $f(t)=A*\cos(\Omega t + \Theta)$, где начальная фаза Θ равномерно распределена на интервале $(0;2\pi)$; б) белый шум; в) фликкер-шум. Подставляя выражения спектральной плотности мощности этих процессов [1] в выражение

(2), получаем, что при гармоническом изменении частоты погрешность изменяется периодически, при белом шуме – пропорциональна времени измерения, при фликкер-шуме – пропорциональна квадрату времени измерения. На практике частота опорного генератора обычно подвержена случайным возмущениям всех трех видов. Поскольку эти события независимы, суммарная дисперсия случайной составляющей погрешности будет равна сумме отдельных составляющих.

Из выражения для набега фазы, пренебрегая случайной составляющей, можно получить значение действительной отстройки частоты поверяемого генератора в момент его коррекции. Рассмотрено два случая, когда систематический уход частоты генератора есть постоянная величина и изменяется по линейному закону. При постоянном характере ухода частоты данные для коррекции получаются при усреднении на всем интервале измерения. Поэтому коррекция происходит на величину, равную среднему значению ухода частоты на интервале измерения. В случае линейного изменения частоты во времени $f_2(t) = \alpha t$ коэффициент α можно оценить по двум точкам [2]: $\alpha = (f_n - f_1)/(n - 1)T$, где f_n – среднее значение ухода частоты на n-м интервале измерения, n – количество интервалов измерения, T – время измерения.

В процессе работы была произведена экспериментальная проверка СКО формирования ШВ синхронометра ЧК7-50. Аналогично ШВ с приемного модуля СРНС в приемнике-компараторе, ШВ с ЧК7-50 использовалась для обмера фазовременным методом характеристик нестабильности опорного кварцевого генератора (КГ). Эти данные использовались для определения вариации Аллана (СКДО) от времени измерения в интервале от 1ч. до 1сут. На рис.2 жирными линиями показаны тренды полученных зависимостей (1 – СКДО для КГ относительно ЧК7-50; 2 – относительно водорода; 3 – СКДО для ЧК7-50 относительно водорода). Как видно из графиков, СКДО ЧК7-50 на порядок меньше чем у КГ на всем интервале времен измерения. Таким образом, мы можем проводить обмер КГ, используя синхронометр ЧК7-50.

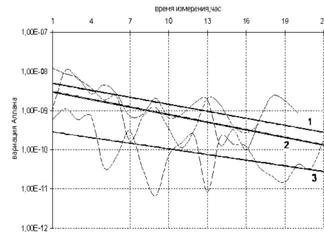


Рис. 2

В процессе работы была составлена обобщенная схема ФВМ измерения отстройки частоты, и получено общее выражение для набега фазы. Методом спектрального анализа получены аналитические выражения, позволяющие оценить вклад каждой компоненты в набег фазы. Получены значения поправок при коррекции частоты поверяемого ОГ по результатам измерения отстройки частоты. Из полученных экспериментальных зависимостей можно сделать вывод, что для данного типа КГ можно производить измерение относительной отстройки частоты при временах измерения 1 час и более.

[1] Пашев Г.П., Рязановский Н.Н., Садовский А.Б.//Вопросы радиоэлектроники. Серия “Радиоизмерительная техника”. 1975. вып. 2. С.13.
[2] Пашев Г.П., Логачев В.А. //Вестник Верхне-Волжского отделения Академии технологических наук РФ. 1995. Вып.1. С.14.

ДИНАМИЧЕСКИЕ МОДЕЛИ ТЕСТОВЫХ ТРАФИКОВ ДЛЯ КОНТРОЛЯ СМО (2)

П.С.Шабалин[1], Л.Ю.Ротков[2], К.Г.Кирьянов[2]

[1] *Нижегородский государственный технический университет,*
[2] *Нижегородский госуниверситет*

В связи с продолжающейся глобальной компьютеризацией самых различных областей науки и техники остаются актуальными рассмотрение и анализ работы систем массового обслуживания (СМО) [1]. Поэтому в настоящей работе продолжено рассмотрение одного из подходов к анализу динамики и взаимосвязи трафиков в модельной системе СМО [2], схемные фрагменты которой широко используются в более сложных системах. Работа направлена на поиск строгих, удобных и наглядных методов анализа характеристик исправности и работоспособности СМО по контролю отклонения от тестовых “профилей” трафиков. Математическая модель (ММ) данной СМО и динамика ее работы исследована в работе [2]. Для примера расчёта тестовых трафиков в этой работе полагалось, что СМО состоит из одной линии передачи данных и нескольких станций, периодически посылающих требования на передачу данных по линии (рис.1). Предполагалось также, что время дискретное и изменяется от 0 до некоторого значения N. В каждый момент времени может обслуживаться только одна заявка с какой-то станции. Если в момент поступления очередного требования на обслуживание линия занята обслуживанием другой заявки, то вновь поступившее требование снимается. Станции работают независимо друг от друга, и в каждый момент времени с определенной вероятностью от любой станции может поступить требование на передачу данных по линии или произойти освобождение линии.

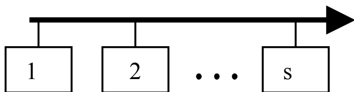


Рис. 1

Программная реализация ММ позволяет получить наглядные представления процессов на выходе каждой станции и на общей линии – определить важные характеристики СМО (время простоя линии, среднее время передачи данных по линии от каждой станции и т.п.). Алгоритм работы данной СМО основан на марковской ММ. Каждая станция в конкретный момент времени может находиться в состоянии “0” или в состоянии “1”. Таким образом, общее число комбинаций состояний станций – 2^s, где s – количество станций в рассматриваемой модели. Каждую

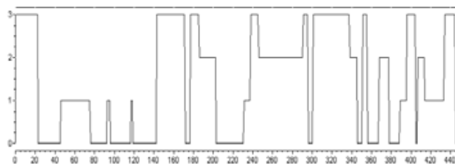


Рис.2. Фрагмент тестовой последовательности на линии (Файл: LINE.txt),когда у всех станций одинаковые вероятности занятия линии (0.086,0.086,0.12) и примерно одинаковые вероятности (0,267,0,267,0,16) освобождения линии после её занятия станцией

такую комбинацию при небольшом количестве станций удобно обозначить числом от 1 до 2^s и использовать эти числа для обозначения состояния на всех станциях одновременно. На основе предположений о марковости в каждый момент времени $t = k + 1$ совокупное состояние всей системы из s станций из какого-либо состояния может перейти из предыдущего состояния в момент времени $t = k$ в любое из 2^s возможных состояний. Вероятность такого перехода в момент времени $t = k + 1$ определяется произведением соответствующей $(2^s \times 2^s)$ – матрицы вероятности переходов на вектор совокупного состояния в момент времени $t = k$.

Практически не трудно при требуемых значениях s построить программно тестовые последовательность любых выбранных пользователем или наиболее важных компонент состояния (станций и линии).

Поэтому для диагностики СМО остаётся снять и проверять сигнатуры [3] или генетические карты [4] тестовых последовательностей.

В заключение отметим, что:

- данный подход может использоваться при анализе работы и диагностике СМО, состоящих из любого количества станций. В общем случае станции могут быть и зависимыми друг от друга. При этом увеличится число состояний системы, усложнится диаграмма переходов, и изменится размерность вероятностной матрицы. Данный способ выбора и задания параметров СМО гарантирует соответствующие вероятностные характеристики реализаций процессов во всех характерных точках системы;
- в силу “аналоговости” ММ (задаваемой вероятностями переходов и т.д.) для получения тестовых трафиков следует выбирать параметры ММ СМО близкие к реально имеющим место на основании априорной информации о работе станций, когда малые локальные отклонения от эталонных трафиков могут приводить к однозначно распознаваемым сигнатурам. Например, на рис.2.показан тестовый трафик на линии, когда у всех трёх станций одинаковые вероятности занятия линии и примерно одинаковые вероятности освобождения линии после её занятия станцией. Для других часто встречающихся случаев (например, первая и вторая станции имеют больше запросов на передачу данных и дольше занимают линию, чем первая станция) желательно иметь свой набор тестовых трафиков.

Работа выполнена при частичной поддержке РФФИ (грант 02-02-17573).

[1] Кофман А., Крюон Р. Массовое обслуживание. Теория и применения. -М.: Мир, 1965.
[2] Шабалин П.С., Ротков Л.Ю., Кирьянов К.Г. Динамические модели тестовых трафиков для контроля СМО (1).
[3] Кирьянов К.Г. К теории сигнатурного анализа. //Техника средств связи. 1980. сер. РИТ, вып.2(27). С.1.
[4] Кирьянов К.Г. Генетический код и тексты: динамические и информационные модели сложных систем. -Нижний Новгород: ТАЛАМ, 2002, 100с.

МАТЕМАТИЧЕСКОЕ ОПИСАНИЕ МОДЕЛЕЙ СЕРТИФИКАЦИИ УДОСТОВЕРЯЮЩИХ ЦЕНТРОВ В ИНФРАСТРУКТУРЕ ОТКРЫТЫХ КЛЮЧЕЙ

А.В.Зобнев, Л.Ю.Ротков, С.В.Соганов

Нижегородский госуниверситет

В настоящее время асимметричная криптография, основывающаяся на открытом распределении ключей, широко используется в различных сферах человеческой деятельности для обеспечения безопасности информационных систем.

Инфраструктура открытых ключей (ИОК) - это комплекс организационно-технических мероприятий и программно-аппаратных средств, необходимых для использования технологии с открытым распределением ключей.

Основной частью ИОК является *система управления сертификатами открытых ключей* объектов в ИОК, базирующаяся на инфраструктуре Удостоверяющих Центров (УЦ). УЦ объединяются в структуры на основе используемой *модели доверительных отношений* (trust model) [1]. Доверие в отношении УЦ означает заверку сертификата одного УЦ электронной цифровой подписью (ЭЦП) другого УЦ.

Различают три модели доверительных отношений УЦ [1]:

- корневая (иерархическая) модель доверия (рис.1);
- сетевая (на основе кросс-сертификации) модель доверия (рис.2);
- смешанная (гибридная) модель доверия.

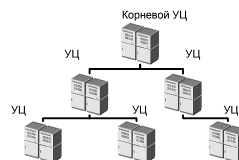


Рис. 1

В *иерархической модели* УЦ высшего уровня заверяют сертификаты УЦ низших уровней. Корневой УЦ имеет самозаверенный сертификат (рис.1). Основное преимущества данной модели – относительная простота масштабирования системы и построения цепочек сертификатов; недостаток – компрометация сертификата УЦ влечет за собой приостановление работы нижестоящих УЦ.

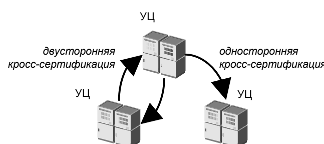


Рис. 2

В *сетевой модели* все УЦ имеют самозаверенные сертификаты, а доверие строится на основе взаимной подписи сертификатов УЦ (кросс-сертификации). Различают *двустороннюю* кросс-сертификацию и *одностороннюю* кросс-сертификацию [1], реализующие, соответственно, взаимное доверие и одностороннее доверие УЦ в сетевой модели (рис.2). Преимущества сетевой модели – система менее уязвима к компрометации сертификатов УЦ; основной недостаток – сложен алгоритм построения цепочек сертификатов.

Гибридная модель доверия представляет из себя объединение иерархической и сетевой моделей в одной инфраструктуре УЦ. В этом случае часть УЦ из иерархии вступают в кросс-сертификацию с УЦ не входящими в иерархию.

Инфраструктура УЦ является базовой подсистемой в ИОК, поэтому актуальным вопросом является исследование и анализ процессов функционирования подсистемы. В контексте данной проблематики важным аспектом является построение адекватной математической модели, описывающей процессы обращения сертификатов объектов ИОК при различных моделях доверительных отношений между УЦ.

Один из возможных вариантов математической модели инфраструктуры УЦ – представление системы в виде графа.

Обозначим множеством $U=\{u_1,u_2,\dots u_n\}$ удостоверяющие центры в системе. Введем на множестве U бинарное отношение R – *“доверяет”* [2]. Тогда, обозначение $u_i R u_j$ для $i,j\in\{1\dots n\}$ означающее, что u_i доверяет u_j (заверка сертификата u_j ЭЦП u_i) можно представить упорядоченной парой (u_i, u_j). Обозначим множеством $E=\{e_1, e_2,\dots e_m\}$ упорядоченные пары (u_i, u_j) для $i,j\in\{1\dots n\}$, тогда направленный граф $G=\{U,E\}$ – будет описывать инфраструктуру УЦ (рис.3).

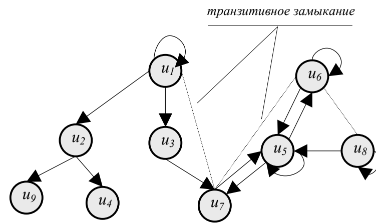


Рис. 3

Можно выделить следующие основные свойства бинарного отношения R – *“доверяет”*:

- *рефлексивность* $(u_i R u_i)$ для корневых УЦ в иерархической модели доверия и для всех УЦ при кросс-сертификации;
- *симметричность* $(u_i R u_j \Rightarrow u_j R u_i)$ при двусторонней кросс-сертификации УЦ;
- *транзитивность* $(u_i R u_j$ и $u_j R u_k \Rightarrow u_i R u_k)$ для всех УЦ.

Таким образом, в терминах представленной модели задача определения доверия пользователя *i-го* УЦ (u_i) пользователю *k-го* УЦ (u_k) будет соответствовать транзитивному замыканию R^* бинарного отношения R для u_i и u_k, т.е. $u_i R^* u_k$, где $R^*\subseteq R$ [2].

Компрометации УЦ u_i в терминах представленной модели будет соответствовать изъятие из множества ребер E графа G ребер, конечной вершиной для которых является u_i .

Сопоставим каждому ребру графа G вес $w(i,j)$, соответствующий степени доверия УЦ u_i УЦ u_j, где $w\in\{w_{\min}\dots\infty\}$. Минимальное значение веса $w_{\min}$ соответствует максимальному доверию, если нет доверия между u_i и u_j, то $w(i,j)=\infty$. В терминах данного представления поиск кратчайшего пути от u_i к u_k по графу будет соответствовать нахождению цепочки сертификатов от *i-го* УЦ к *k-му* УЦ с наибольшей степенью доверия. Для построения цепочек сертификатов с максимальным доверием можно использовать алгоритм Дейкстры [2].

[1] Microsoft Windows Server 2003 Deployment Kit. Online. http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/.

[2] Свами М., Тхуласираман К. Графы, сети и алгоритмы. -М.: Мир, 1984, 455с.

ОБРАБОТКА ДАННЫХ В ЗАДАЧЕ МОНИТОРИНГА ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ РЕГИОНА

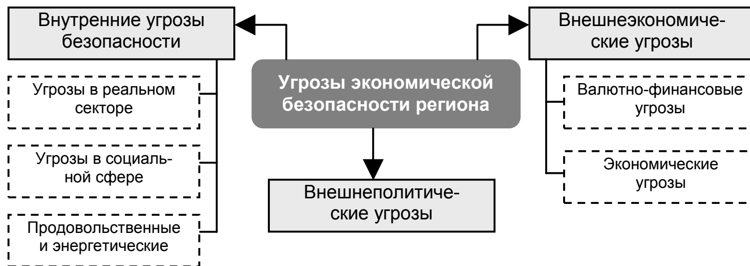
А.Н.Голубцов[1], А.В.Зобнев[2], С.В.Мацур, С.В.Соганов[3]

[1]Нижегородский областной комитет государственной статистики,

[2]Нижегородский госуниверситет, [3]НФ ФГУП НТЦ “Атлас”

Мониторинг экономической безопасности региона в широком смысле заключается в сборе необходимых данных и их последующей аналитической обработке.

Одной из основных проблем при построении системы мониторинга является выбор необходимых макропоказателей, характеризующих социально-экономическое состояние региона. Выбор показателей осуществляется на основе структуры угроз экономической безопасности (рис.).



Автоматизированная система мониторинга экономической безопасности должна состоять, как минимум, из следующих подсистем и модулей.

1) **Подсистема сбора и обработки данных**.

Входными данными для подсистемы выступают массивы информации, содержащие в себе различные финансовые отчеты, результаты социологических опросов, рейтингов и прочие необходимые данные. Модуль трансформации данных по определенным алгоритмам переносит эти “сырые” данные в единое хранилище. Хранилище данных здесь понимается в терминах технологии OLAP [1].

2) **Подсистема аналитической обработки данных.**

Решает широкий круг вопросов в части аналитической обработки и оценки состояния региона с использованием различных OLAP средств [1], методов статистического и разведочного анализа данных (Data Mining [1]). На вход подсистемы поступает информация из хранилища данных. Подсистема аналитической обработки может содержать в себе цифровые интерфейсы для доступа сторонних аналитиков и экспертов к хранилищу данных, при этом должно осуществляться разграничение доступа субъектов к информации в хранилище данных.

В настоящее время достаточно перспективным направлением является использование ситуационного анализа и ситуационных центров в задачах мониторинга сложных социально-экономических систем и прогнозирования их развития. Ситуа-

ционный центр [2] – это программно-аппаратный комплекс, осуществляющий адекватное представление оперативной информации из хранилища данных и позволяющий, на основе модели системы, осуществлять прогнозирование ситуаций. Для целей ситуационного анализа необходимо построить адекватную математическую модель поведения системы. Данная задача достаточно сложна, требует длительных научных изысканий на стыке математического анализа и эконометрики.

Кроме ситуационного анализа данных в сложных системах различной природы, в том числе и социально-экономических системах, возможно использование методов морфологического анализа. Данный метод при корректном ранжировании результатов расстановки весов может достаточно адекватно отражать динамику сложной системы и позволяет оценивать состояние системы на временных срезах.

Ниже представлены некоторые критериальные оценки социально-экономического состояния региона, построенные на основе методов морфологического анализа.

Дельта-оценка безопасности формируется на основе сравнения текущих значений макропоказателей – W_i с их пороговыми значениями W_i^*. При этом учитываются веса макропоказателей – λ_i, указывающие степень влияния конкретного макропоказателя на экономическую безопасность региона. Дельта-оценка социально-экономического состояния региона Ψ определяется выражением

$$\Psi = \sum_{i \in (1,N)} \lambda_i \cdot \delta(W_i, W_i^*) ,$$

где $\delta(W_i, W_i^*)$ – степень отклонения макропоказателя от порога.

Оценка стабильности региона [3] характеризует текущее состояние устойчивости региона к изменениям макропоказателей. Вектор оценок ущерба $\vec{V}$ определяется выражением

$$\vec{V} = \left\{ \sum_{i \in (1,N)} \lambda_i \cdot \nu_{i,j} \right\} ,$$

где $\nu_{i,j}$ – оценка величины регионального ущерба при единичном увеличении W_i и одновременном единичном уменьшении W_j.

[1] Елманова Н., Федоров А. Введение в OLAP-технологии Microsoft. -М.: Диалог-Мифи, 2002, 268с.

[2] Бекренев В. Ситуационные центры и социально-экономическое моделирование. //Управление персоналом. 2000. №12.

[3] Кульба В.В. и др. Проблемы обеспечения экономической безопасности сложных социально-экономических систем. –М.: Изд-во ИПУ РАН, 2000.

О СВЯЗИ РАССТОЯНИЯ ЕДИНСТВЕННОСТИ ШЕННОНА С БАЗОВЫМИ ПАРАМЕТРАМИ ШИФРОТЕКСТА

К.Г.Кирьянов, А.А.Горбунов

Нижегородский госуниверситет

В одной из первых теоретических работ в области криптографии К. Шенноном была предложена математическая модель случайного шифра, и рассмотрен в статистическом плане подход к оценке его криптостойкости [1]. При введении понятия случайного шифра (см. рис.) Шеннон сделал следующие допущения:

- число возможных дискретных сообщений $M = \{m_1, m_2, \ldots, m_N\}$ открытого текста длины *N* равняется числу возможных криптограмм $C = \{c_1, c_2, \ldots, c_N\}$ длины *N*;
- имеется *k* равновероятных ключей (криптосистем) *K*, причем каждое открытое сообщение взаимнооднозначно преобразуется в конкретную криптограмму при помощи единственного ключа;
- каждой криптограмме соответствует случайный набор *k* возможных открытых сообщений;
- все возможные исходные сообщения разделяются на две группы: высоковероятную и низковероятную, что определяется избыточностью языка открытого текста.

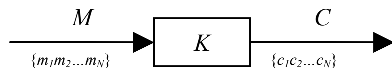
В качестве теоретической меры секретности используется условная энтропия ключа (мера неопределенности) при условии известной криптограммы *C*, названная Шенноном *ненадежностью*. При большом числе ключей, определяющих отображение сообщений высоковероятной группы в область криптограмм, в [1] с учетом указанных выше предположений показано, что функция ненадежности равняется

$$H_C(K) \cong H(K) - DN \,, \qquad (1)$$

где $D = \log L - \dfrac{H(M)}{N}$ – избыточность открытого сообщения на один символ, $H(K)$ – энтропия ключа, $H(M)$ – энтропия открытого сообщения *M* длины *N*, *L* – размерность алфавита открытого сообщения и криптограммы.

Значение длины криптограммы *N*, при которой только у одного из сообщений высоковероятной группы вероятность остается близкой к единице, а вероятности всех остальных сообщений стремятся к нулю, называется *расстоянием единственности*. Данная величина, соответственно, равна [1, 2]

$$n_0 = \frac{H(K)}{D} \,. \qquad (2)$$



С другой стороны, шифратор можно рассматривать просто как генератор текстового сигнала *C*. Находясь в неавтономном режиме, на входе он испытывает воздействие сигнала открытого текста, а на выходе выдает сигнал шифротекста. Символы

ключа при этом фигурируют в качестве параметров математической модели (ММ) данного дискретного автомата.

В [3] для идентификации дискретного автомата по его выходному тексту введен набор *базовых параметров* (БП) ММ источника текста:

$$\text{БП} = (q, n). \tag{3}$$

Здесь q – число уровней квантования, n – “сложность” порождающего источника. При этом предполагается, что для каждого i-го участка стационарности длиной m_i существует стационарный абстрактный детерминированный дискретный автомат n-го порядка, являющийся источником участка текста, который может безошибочно породить по его n начальным символам все оставшиеся m_i–n символов i-го участка текста. Средняя длина участка стационарности текста (средняя длина “гена”) оценена теоретически [3] и составляет:

$$\overline{m} = (q^n)^{1/2}. \tag{4}$$

После логарифмирования обеих частей равенства (4) получаем следующее выражение для параметра n:

$$n = \frac{\log(\overline{m})}{\log(q^{1/2})}. \tag{5}$$

В [3] за оценку избыточности текста взята величина

$$D = \frac{1}{2} \cdot \log q. \tag{6}$$

Поэтому при q=L и $H(K) = \log(\overline{m})$ получаем формулу (7) для расстояния единственности Шеннона, аналогичную (2) в терминах базовых параметров шифротекста:

$$n = \frac{\log(\overline{m})}{D}. \tag{7}$$

Работа выполнена при частичной поддержке РФФИ (грант 02-02-17573).

[1] Шеннон К. Теория связи в секретных системах. Работы по теории информации и кибернетике. Пер. В.Ф. Писаренко. –М.: ИЛ, 1963. с.333.
[2] Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография. –СПб.: Лань, 2000.
[3] Кирьянов К.Г. // В кн.: Труды 3-й межд. конф. “Идентификация систем и задачи управления” SICPRO′04. М.: ИПУ РАН, 2004, с.187.

ИММУНОЛОГИЧЕСКИЙ ПОДХОД К ОБНАРУЖЕНИЮ ВТОРЖЕНИЙ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

С.В.Корелов

Нижегородский госуниверситет

Природные иммунные системы защищают животных от чужеродных микроорганизмов. Роль компьютерных систем безопасности аналогична. Однако последние далеко не так совершенны, как их биологические аналоги. И все же можно предпринять попытку реализовать некоторые свойства иммунной системы в обнаружении чужеродных организмов на искусственном уровне, создав искусственную иммунную систему для компьютера. Иммунологами проблема, решаемая иммунной системой, традиционно описывается как задача распознавания "своих" и "чужих" и устранения последних. Проблема защиты компьютерных систем может быть также представлена как задача распознавания "своих" и "чужих". В этом случае "чужие" могут быть представлены как неавторизованные пользователи, чужеродный код в виде вирусов, несанкционированные процессы и т.п.

Распознавание между "своими" и "чужими" в биологической иммунной системе затруднено рядом проблем. Во-первых, компоненты тела построены из такого же материала, как и чужеродные организмы. Во-вторых, объем решаемой задачи велик по сравнению с внутренними ресурсами. Трудность такой задачи распознавания подтверждается наличием ошибок. Но биологические иммунные системы имеют ряд отличительных признаков, использование которых может существенно облегчить построение системы обнаружения вторжений. Такими чертами являются многоуровневая защита, распределенность обнаружения, разнообразие между различными системами и непосредственно сам процесс обнаружения [1]. Рассмотрим, как эти черты проявляются в компьютерных системах.

Многоуровневая защита. Многие компьютерные системы монолитны. Редко, когда находится резервная копия механизма защиты в случае нарушения работоспособности первой копии.

Распределенность обнаружения. Подсистемы обнаружения и памяти иммунной системы сильно распределены. Не существует централизованного управления этими подсистемами, однако их успешная деятельность обуславливается сильными связями между отдельными детекторами и нервными окончаниями.

Каждая копия системы обнаружения уникальна. Каждый индивидуум в популяции имеет свой уникальный набор клеток и молекул для защиты. Системы компьютерной безопасности зачастую защищают несколько копий программного обеспечения. Если защита будет уязвлена, то такой уязвимости будут подвержены все копии программного обеспечения. Лучшим подходом к организации защиты было бы обеспечение каждого участка своим уникальным набором детекторов (или даже своей копией программы защиты). Таким образом, если одна копия будет скомпрометирована, то остальные смогут поддержать требуемый уровень безопасности.

Обнаружение незнакомых чужеродных организмов. Иммунная система, которая защищает нас от тех видов чужеродных организмов, которые ей известны, ме-

нее эффективна, чем система, способная распознавать новые виды. Она помнит предыдущие воздействия и вырабатывает на них более агрессивный ответ. Иммунологи называют это вторичной реакцией. Однако в случае неизвестной инфекции возникает первичная реакция иммунной системы. Она начинает вырабатывать новые детекторы, способные обнаружить данные чужеродные организмы. Данный процесс медленнее, чем вторичная реакция, однако она предусматривает устранение недостатка, присущего многим системам защиты.

Несовершенство обнаружения. Не все антигены хорошо распознаются заранее подготовленными детекторами. Однако иммунная система использует два пути решения данной проблемы: обучение и распределенность обнаружения.

На основе данных черт иммунной системы можно построить искусственную систему со следующими основными свойствами: четкое описание “своих”, предотвращение или обнаружение и уничтожение несанкционированных процессов, запоминание предыдущих фактов вторжения, наличие метода распознавания новых вторжений и наличие метода защиты самой себя.

Данный подход можно применить к защите программ в компьютерной системе. Так описание поведения программы можно построить на основе ее системных вызовов. Необходимо создать базу данных последовательностей системных вызовов конкретной программы при ее нормальной работе. Каждая база будет специфична к конкретной архитектуре, версии программного обеспечения и конфигурации и т.п. Если последовательность системных вызовов наблюдаемой программы не будет соответствовать базе нормального поведения, то можно сделать предположение об ее аномальном поведении.

[1] Forrest S., Hofmeyr S., and Somayaji A. //Communications of the ACM. 1997. 40(10). P.88.
[2] Watkins A. An Immunological Approach to Intrusion Detection. //In: 12th annual Canadian information technology security symposium. 2000.
[3] D’Haeseleer P. An immunological approach to change detection: Theoretical results. //In: Proceedings of the 9th IEEE Computer Security Foundations Workshop. Los Alamitos, CA, 1996.

АНАЛИЗ СУЩЕСТВУЮЩИХ CMS WEB-САЙТОВ И ПРЕДЛОЖЕНИЯ ПО РАЗРАБОТКЕ УНИВЕРСАЛЬНОЙ CMS

Л.Л.Давыдов[1], А.А.Рябов[2]

[1] *Нижегородский Государственный Технический Университет*
[2] *Нижегородский госуниверситет*

Количество WEB-сайтов растет в геометрической прогрессии, растут объемы и характер информации, и, как следствие, возникает проблема организации и структурирования этой информации на Интернет-ресурсах.

Чтобы расширить возможности по представлению различного рода информации в сеть Интернет, разрабатываются специальные системы управления информацией на WEB-ресурсах – CMS (Content Management System).

В настоящее время использование CMS – один из самых эффективных способов переноса бизнес процессов в сеть Интернет. С помощью систем подобного рода перенос информации на WEB-сайт становится наиболее доступным и оперативным. CMS представляют собой программное обеспечение, ориентированное на обычного пользователя, использование которого не требует получения специализированных знаний в области информационных технологий.

Все современные CMS строятся примерно по одинаковому принципу (рис.1). У любой CMS есть администраторская часть, доступ к которой имеют сотрудники организации, в чьем ведении находится WEB-сайт, и пользовательская часть, доступная для пользователей из сети Интернет. Администраторская часть состоит из набора модулей – стандартных блоков, из которых состоит любой сайт (лента новостей, опрос, каталог товаров, статья, гостевая книга и т.д.). Основными характеристиками современных CMS является:

- количество и характер встроенных модулей;
- набор средств, с помощью которых организована CMS (web-сервер, СУБД, язык скриптов CMS);
- многопользовательская или однопользовательская система;
- наличие различных уровней доступа к CMS (администратор, модератор, гость).

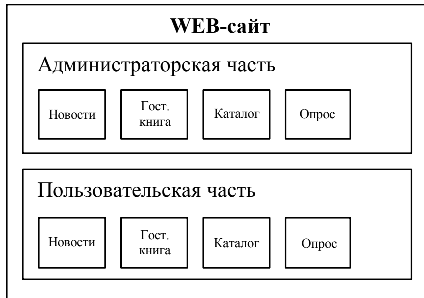


Рис. 1

С помощью администраторской части сайта можно добавлять в структуру сайта различные разделы, но характер добавляемых разделов ограничивается набором модулей, встроенных в CMS. Например, если администратору сайта понадобилось расширить функциональность сайта и добавить на него форум, а такого модуля не встроено в CMS, которую использует организация, придется прибегнуть к услугам компании, разработавшей WEB-сайт, т.к. совместимых CMS в настоящее время не существует. Если организация захочет обратиться к другой компании, оказывающей услуги по разработки WEB-сайтов, она будет вынуждена переходить на другую CMS, что заведомо дороже, чем разработка одного требуемого модуля.

Также проблемой современных CMS является отсутствие возможности легкого изменения дизайнерского решения сайта, причем даже самого незначительного. Так как дизайн сайта является важной составляющей эффективности его использования, очень важна возможность его менять, а также адаптировать под различные нужды.

Проанализировав преимущества и недостатки существующих CMS, можно сделать вывод, что в настоящее время встает проблема универсальности современных CMS, их более удобного использования.

Для разрешения проблемы легкой смены дизайна сайта, предлагается встраивать в CMS редактор шаблонов, доступный для пользователя, не имеющего глубо-

ких знаний Интернет-технологий. Таким образом, можно будет решить проблему легкой смены дизайна сайта без дополнительного обращения к компаниям-разработчикам WEB-сайтов. При помощи администраторского интерфейса администратор сайта сможет загружать шаблоны для различных страниц сайта, быстро и удобно изменяя его, что позволит получить экономию времени и денежных средств на последующую работу с сайтом.



Рис. 2

Для решения проблемы быстрого внедрения на сайт модулей, не предусмотренных при начальной разработке CMS сайта, предлагается встраивать конструктор модулей (рис. 2), с помощью которого администратор сайта своими силами сможет разработать и установить на сайт новый раздел, основанный на разработанном модуле (например, модуль форума).

Организация, пользующаяся CMS, оснащенной конструктором модулей и редактором шаблонов, сможет значительно повысить эффективность работы с WEB-сайтом путем сокращения расходов на дополнительные дорогостоящие разработки на 30% и повышения оперативности обновления информации на WEB-сайте.

ПОИСК ТИПОВЫХ АЛГОРИТМОВ В ИСПОЛНЯЕМЫХ КОДАХ ПРОГРАММ

Д.Л.Туренко, А.В.Корюкалов

Нижегородский госуниверситет

В данной работе рассмотрен один из подходов к решению задачи нахождения заданного типового алгоритма в исполняемом модуле программы. В качестве исследуемой аппаратно-программной среды выбрана наиболее распространенная платформа ПЭВМ с процессором Intel x86 под управлением операционных систем семейства Microsoft Windows 9x/NT.

Предлагается следующий подход к решению данной задачи. В соответствии с [1] программно реализован алгоритм построения орграфа вызовов и переходов по последовательности машинных команд исполняемого модуля прикладного программного интерфейса Win32. С помощью разработанных программных средств выполняется построение орграфов $G_i=(X_i, R_i)$ (где X_i – множество вершин, R_i – множество ребер) исследуемого исполняемого модуля ($i = 1$) и типового алгоритма ($i = 2$), например такого, как алгоритм сортировки массива или алгоритм криптографического преобразования.

Таким образом, задача поиска алгоритма в программе сводится к поиску вложения орграфа G_2 в орграф G_1, т.е. построению отображения $\varphi: G_2 \to G_1$ со следующими свойствами:

1) $\forall a,b \in X_2, a \neq b \Rightarrow \varphi(a) \neq \varphi(b)$
2) если $(a,b) \in R_2$, то $(\varphi(a), \varphi(b)) \in R_1$

Для построения искомого отображения $\varphi: G_2 \rightarrow G_1$ программно реализован алгоритм [2] распознавания изоморфного вложения одного орграфа в другой с некоторыми изменениями. Данный алгоритм основан на методе "расширения" начального (пустого) множества вершин X_1 большого орграфа G_1 до максимально возможного (тупикового) множества, которое определяет в орграфе G_1 подграф, изоморфный графу G_2. Если свойства 1-2 не выполняются, то попытка построить тупиковое подмножество повторяется до тех пор, пока не будут исчерпаны все варианты.

В результате работы данного алгоритма строится множество $\Phi = \{\varphi_i\}$ всех возможных отображений $\varphi_i: G_2 \rightarrow G_1$ со свойствами 1-2. Если множество Φ – пустое, то делается вывод, что типовой алгоритм, соответствующий орграфу G_2 не является частью исследуемой программы.

Тестирование разработанных программных средств проводилось для небольшой консольной программы API Win32 и алгоритма сортировки массива целых чисел. В консольную программу была включена вышеуказанная функция сортировки. С помощью разработанных программных средств были построены орграфы $G_1=(X_1, R_1)$ ($|X_1|$=760) и $G_2=(X_2, R_2)$ ($|X_1|$=12) и найдено требуемое отображение $\varphi: G_2 \rightarrow G_1$.

Для фиксированного алгоритма A может быть построен целый класс орграфов $G(A)$, что зависит от языка программирования, стиля программирования, настроек компилятора и других факторов. Поэтому необходимо определить преобразование $d: G(A) \rightarrow G_A$, которое ставит в соответствие классу $G(A)$ эталонный орграф G_A алгоритма A. При этом должны выполняться следующие условия:

- $\forall G_1, G_2 \in G(A)\ d(G_1)=d(G_2)=G_A$
- $\forall A_1 \neq A_2 \Rightarrow G_{A1} \neq G_{A2}$
- (если $G_1 \in G(A_1)$, $G_2 \in G(A_2)$, то $\exists$ отображение $\varphi: d(G_2) \rightarrow d(G_1)$ со свойствами 1)-2)$\Leftrightarrow$ (алгоритм A_2 является частью алгоритма A_1)

Преобразование d определяет некие критерии похожести, т.е. допущения, при которых различные орграфы можно считать орграфами одного и того же алгоритма.

Исследования в данной области будут продолжены и направлены, в первую очередь, на определение свойств преобразования d с целью совершенствования данного подхода к решению задач идентификации алгоритмов программ.

[1] Туренко Д.Л., Кирьянов К.Г. //В кн.: Тр. 6-й научн. конф. по радиофизике./Ред. А.В.Якимов. –Н.Новгород: ТАЛАМ, 2002, с.328

[2] Нечепуренко М.И., Попков В.К., Майнагашев С.М. и другие. Алгоритмы и программы решения задач на графах и сетях. -Новосибирск: Наука. Сибирское Отделение, 1990.